# SYSTEM AND METHOD FOR PROVIDING SECURITY IN A TELECOMMUNICATION NETWORK

## CROSS-REFERENCE TO RELATED APPLICATIONS

This application is filed concurrently with the following commonly-owned applications:

SYSTEM AND METHOD FOR MAINTAINING A COMMUNICATION LINK, Attorney Docket 062891.0293;

SYSTEM AND METHOD FOR ENABLING MULTICAST TELECOMMUNICATIONS, Attorney Docket 062891.0297; and

SYSTEM AND METHOD FOR A VIRTUAL TELEPHONY INTERMEDIARY, Attorney Docket 062891.0381.

## TECHNICAL FIELD OF THE INVENTION

This invention relates generally to the field of telecommunications, and more specifically to a system and method for providing security in a telecommunication network.

BACKGROUND OF THE INVENTION

Historically, telecommunications have involved the transmission of voice and fax signals over a network dedicated to telecommunications, such as the Public Switched Telephone Network (PSTN) or a Private Branch Exchange (PBX). Similarly, data communications between computers have also historically been transmitted on a dedicated data network, such as a local area network (LAN) or a wide area network (WAN). Currently, telecommunications and data transmissions are being merged into an integrated communication network using technologies such as Voice over Internet Protocol (VoIP).

Since many LANs and WANs transmit computer data using Internet Protocol (IP), VoIP uses this existing technology to transmit voice and fax signals by converting these signals into digital data and encapsulating the data for transmission over an IP network. Furthermore, by using existing "long distance" computer networks, such as private (or leased) WANs or the Internet, telephone calls can be made to distant locations using VoIP without incurring long distance telephone charges. For example, an employee of a company in Dallas can call a co-worker who is based in San Jose using the company's existing WAN. However, if these long distance communications are made over untrusted networks, or if calls are received from untrusted locations, security problems arise. These security issues exist when using VoIP since the IP telephones are connected to the same networks as computers containing sensitive information.

SUMMARY OF THE INVENTION

In accordance with the present invention, a system and method for providing security in a telecommunication network are provided that substantially eliminate or reduce disadvantages or problems associated with previously developed systems and methods. In particular, the present invention contemplates an authentication controller capable of evaluating incoming telecommunications, and a telephony proxy capable of serving as an intermediary to enable a telephone call between a trusted telephone and an untrusted device.

In one embodiment of the present invention, a method is provided for establishing a telephone call between a trusted Internet Protocol (IP) telephone and an untrusted device. The method includes receiving a call initiation request from the untrusted device that indicates a desired communication with the trusted IP telephone. The method evaluates the call initiation request, and establishes a telecommunication link between the untrusted device and the trusted telephone in response to a positive evaluation of the call initiation request.

In another embodiment of the present invention, a communication network is provided for establishing a telephone call between a trusted telephone and an untrusted device. The communication network includes a first trusted network and a trusted telephone coupled to the first trusted network. The communication network also includes an authentication controller coupled to the first trusted network and operable to evaluate a call initiation request received from an untrusted device external to the first trusted network. The call initiation request indicates a

desired communication with the trusted telephone. The network further includes a call manager operable to initiate the creation of a telecommunication link between the trusted telephone and the untrusted device in response to a positive evaluation of the call initiation request.

Technical advantages of the present invention include a system and method for providing security in a telecommunication network. The present invention allows telecommunications between a trusted telephone coupled to a protected network and an untrusted device external to the protected network to occur while still maintaining network security. The present invention can be used to evaluate incoming telecommunications based on a number of factors, including, but not limited to, the source and/or destination of the telecommunications, the transmission format of the telecommunications, and the compression format of the telecommunications.

The present invention may also provide a telephony proxy that serves as an intermediary between the trusted telephone and the untrusted device. The telephony proxy can be implemented in various forms, such as software or embedded firmware for incorporation into hardware such as routers and firewalls. The telephony proxy may also be used to manipulate the media streaming between the trusted telephone and the untrusted device as required to maintain the integrity of the protected network. Other technical advantages are readily apparent to one skilled in the art from the following figures, descriptions, and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention, and for further features and advantages, reference is now made to the following description, taken in conjunction with the accompanying drawings, in which:

FIGURE 1 illustrates an exemplary communication network in accordance with the present invention;

FIGURE 2 illustrates an exemplary telecommunication link between network devices using a virtual telephony device in accordance with the present invention; and

FIGURE 3 illustrates an exemplary method for establishing a telephone call between a trusted telephone and an untrusted device in the communication network of FIGURE 1.

DETAILED DESCRIPTION OF THE INVENTION

FIGURE 1 illustrates an exemplary communication network 10. In the illustrated embodiment, communication network 10 includes a plurality of local area networks (LANs) 20, 30, 40 that are interconnected using various techniques, including the Internet 50 and a wide area network (WAN) 60. Each LAN is a computer data network that is further operable to transmit audio and/or video telecommunication signals. Communication network 10 also includes a remote communication site 70 coupled to one or more of LANs 20, 30, 40 using the Public Switched Telephone Network (PSTN) 80. Although a specific communication network is illustrated in FIGURE 1, the term "communication network" should be interpreted as generically defining any network or combination of networks capable of transmitting telecommunication signals, data, and/or messages.

In a particular embodiment, LANs 20, 30, 40 are Ethernet networks that transmit data using the Internet Protocol (IP). However, LANs 20, 30, 40 may be any type of network that allows the transmission of audio and/or video telecommunication data, as well as traditional computer data. Therefore, although subsequent description will be primarily focused on IP networks, it should be understood that other appropriate networks including, but not limited to, Frame Relay networks, Asynchronous Transfer Mode networks, and Token Ring networks are also included within the scope of this description.

As mentioned above, LANs 20, 30, 40 are coupled to each other using other IP networks. For example, LAN 20 is coupled to LAN 30 using Internet 50, which is a public IP network. Similarly, LAN 20 is coupled to LAN 40 though WAN

60, which is typically a semi-private IP network (such as a set of communications lines owned by a telecommunication company and leased to various businesses). Remote site 70 may be coupled with LANs 20, 30, 40 using Internet 50 and/or PSTN 80. Remote site 70 may be directly connected to Internet 50, or it may use PSTN 80 to send data to and receive data from Internet 50 using an Internet Service Provider (ISP) 90. Furthermore, remote site 70 may be coupled to a LAN, such as LAN 20, using only PSTN 80. In this case, a gateway 22 facilitates communications between telephony devices at remote site 70 and LAN 20 by converting between the different data transmission formats (e.g., audio compression and encoding formats) utilized by LAN 20 and PSTN 80.

IP networks transmit data (including voice and video data) by placing the data in packets and sending each packet to the selected destination. Unlike a circuit-switched network (e.g., PSTN 80), dedicated bandwidth is not required for the duration of a call or fax transmission over LANs 20, 30, 40, Internet 50 or WAN 60. Instead, each network device sends packets across the network as they become available for transmission. This feature makes bandwidth available for other transmissions when voice or fax data is not being transmitted.

IP telephony devices, such as an IP telephone, can be coupled to any of these IP networks and used for communication between users of the networks. Furthermore, since all IP networks share a common method of transmitting data, telecommunication signals may be transmitted between telephony devices that are located on different, but interconnected, IP networks. The technology that allows

telecommunications to be transmitted over an IP network may be referred to as Voice over IP (VoIP). As an example, IP telephony devices 24 are coupled to LAN 20 to allow communication over LAN 20. IP telephony devices 24 have the capability of encapsulating a user's voice (or other inputs, such as the user's image) into IP packets so that the voice can be transmitted over LANs 20, 30, 40, Internet 50, WAN 60, and/or PSTN 80. IP telephony devices may include telephones, fax machines, computers running telephony software (such as MICROSOFT NETMEETING), gateways, or any other device capable of performing telephony functions over an IP network. For the purposes of this application, all types of telephony devices (both IP and non-IP) will be referred to as "telephones."

One example of an IP telephone is an IP Ethernet telephone that plugs directly into an Ethernet RJ-45 jack, as opposed to a traditional RJ-11 telephone jack. Alternatively, a user may plug a handset or headset directly into a personal computer on an IP network to form a virtual IP telephone. An IP telephone typically resembles a traditional digital PBX telephone, but instead of connecting to a proprietary PBX port, the telephone has an IP port, such as an Ethernet port. An IP telephone operates as a standard IP network device and typically has its own IP address (IP telephones may also have more than one IP address). IP telephones may also have the ability to handle data coding and decoding at the telephone. This feature allows the telephone to switch compression schemes on demand, such as switching between G.711 and G.723 compression.

A call manager 26 controls IP telephones 24 on LAN 20.

Call manager 26 is an application that controls call processing, routing, telephone features and options (such as call hold, call transfer and caller ID), device configuration, and other telephony functions and parameters within communication network 10. Call manager 26 can control all of the IP telephones 24 on LAN 20, and it may also control IP telephones on other IP networks. For example, call manager 26 is capable of controlling IP telephones 32 on LAN 30 and IP telephones 42 on LAN 40.

When a user wishes to place a call from an IP telephone 24a on LAN 20 to another IP telephone 24b on LAN 20 (an intra-LAN call), the calling telephone transmits a signal to call manager 26 indicating the desired function and the telephone to be called. Call manager 26 then checks on the availability of the called telephone and, if available, establishes the call by instructing the calling (originating) telephone to begin audio and/or video (media) streaming to the called (destination) telephone. The initial signaling between call manager 26 and either the originating telephone or the destination telephone is transmitted over LAN 20 using the Transmission Control Protocol (TCP). The TCP network layer in the transmitting telephone divides the data to be transmitted into one or more packets, numbers the packets, and then forwards them to the IP network layer for transmission to the destination telephone. Although each packet has the same destination IP address, the packets may travel along different paths to reach the intended destination. As the packets reach the destination telephone, the TCP layer of the destination telephone reassembles the individual packets and ensures that they all have arrived. Once TCP reassembles the data,

it forwards the data to the destination telephone as a single message.

After call manager 26 initiates the call with signaling via TCP, audio streaming between the telephones begins. A codec (coder/decoder) converts the voice, video or fax signals generated by the users of the telephones from analog voice signals into digital form. The codec may be implemented either in software or as special-purpose hardware in IP telephones 24. In the case of an IP telephone, as the user speaks into the handset, the codec converts the analog voice signals into digital data. The digitally encoded data is then encapsulated into IP packets so that it can be transmitted over LAN 20.

The encapsulation of audio and video streams between IP telephones 24 may be performed using Real-Time Transport Protocol (RTP) running over User Datagram Protocol (UDP), or any other suitable communication protocol. As with TCP, UDP uses the Internet Protocol to get data packets from one computer to another. Unlike TCP, however, UDP does not provide sequencing and error-checking of the arriving packets. However, since UDP does not perform these functions, UDP operates faster than TCP and is useful when speed is more important than accuracy. This is true of audio and video streaming since it is critical that the data be transmitted as quickly as possible, but it is not critical that every single packet is reassembled correctly (either its absence is negligible or its content can be extrapolated by the destination telephone).

Once the UDP network layer has received and reassembled the IP packets at the destination telephone, a codec in the destination telephone translates the digital

data into analog audio and/or video signals for presentation to the user. The codec may be implemented either in software or as special-purpose hardware in IP telephones 24. The entire process is repeated each time that any call participant (or any other source) generates an audio, video, or fax signal.

In addition to intra-LAN telephone calls, calls can also be placed to and received from non-IP telephones that are connected to PSTN 80, such as telephone 74 located at remote site 70. Such calls are made through gateway 22. Gateway 22 converts analog or digital circuit-switched data transmitted by PSTN 80 to packetized data transmitted by LAN 20, and vice-versa. When voice data packets are transmitted from LAN 20 to remote site 70 over PSTN 80, gateway 22 retrieves the data contained in the packets coming from LAN 20 and converts this digital data to the analog or digital format used by the PSTN trunk 82 to which gateway 22 is coupled. Since the digital format used for voice transmissions over an IP network is often different than the format used on the digital trunks of PSTN 80, the gateway provides conversion between these different digital formats, referred to as transcoding. Gateway 22 also translates between the VoIP call control system and the Signaling System 7 (SS7) protocol or other signaling protocols used in PSTN 80.

For voice transmissions from remote site 70 back to LAN 20 over PSTN 80, the process is reversed. Gateway 22 takes the incoming voice transmission (in either analog or digital form) and converts it into the digital format used by LAN 20. The digital data is then encapsulated into IP packets and transmitted over LAN 20. This process is

continued between PSTN 80 and LAN 20 through gateway 22 until the call is complete.

Remote site 70 may also include an IP telephone 72. A call may be placed between telephone 72 and another IP telephone 24 on LAN 20 using Internet 50 and ISP 90. Telephone 72 is connected to a computer 76 that is coupled to ISP 90 using a modem. IP-encapsulated audio and/or video data packets are sent from telephone 72 to computer 76. Computer 76 then uses the modem to transmit the data over PSTN to ISP 90, where the data is transmitted to Internet 50 (alternatively, computer 76 may be directly connected to Internet 50). The data is finally transmitted over Internet 50 to LAN 20, where it is received by telephone 24. Note that no gateway 22 is required, since the communication is between two IP telephones (even though the telephones are not directly connected).

Calls can also be made between an IP telephone located on LAN 20 and an IP telephone located on another LAN 30, 40, on Internet 50, or on WAN 60. For example, a call may be placed between IP telephone 24 connected to LAN 20 and IP telephone 42 connected to LAN 40. As discussed above, the analog voice or fax data is digitized and encapsulated into IP packets at the originating IP telephone 24. A router (or other similar device) then directs the packets over WAN 60 to the IP address of the destination IP telephone 42. IP telephone 42 then retrieves the data and coverts it to analog form for presentation to the user. IP telephone 42 may be controlled by the same call manager 26 as IP telephone 24, or it may be controlled by a call manager on LAN 30 or LAN 40.

In any of the above scenarios, when a call is placed

to an IP telephone, for example IP telephone 24, a call initiation request is first sent to call manager 26. If the originating telephone is an IP telephone (e.g., a telephone on LAN 30, LAN 40, Internet 50, or WAN 60), the originating IP telephone generates the call initiation request and sends the request to call manager 26. If the originating telephone is a non-IP telephone, such as telephone 74, gateway 22 first intercepts the incoming call from PSTN 80, and then sends a call initiation request to call manager 26 indicating the IP telephone that is being called. In either case, once call manager 26 receives the call initiation request, call manager 26 sends a signal to the destination IP telephone offering the call to the telephone.

If the destination telephone, for example, IP telephone 24, can accept the call (e.g., it is not in use or under a Do Not Disturb instruction from the user), IP telephone 24 replies to call manager 26 that it will accept. Upon receiving this acceptance, call manager 26 transmits a signal to IP telephone 24 to cause it to ring. The telephone's user can then hear the ring and can take the telephone "off-hook" to receive the call. Taking the telephone off-hook may include, but is not limited to, picking up a handset, pressing the ringing line's button, pressing a speakerphone button, or otherwise indicating that the telephone is ready to receive the incoming call. For the purposes of this application, the term "off-hook" is used to generically indicate a condition of a telephone when it is ready to initiate or receive telecommunication signals. Once IP telephone 24 has been taken off-hook, call manager 26 establishes media streaming (such as RTP media streaming) between IP telephone 24 and the originating

telephone. If the originating telephone is a non-IP telephone, such as telephone 74, the media streaming occurs between IP telephone 24 and gateway 22. Gateway 22 then transmits the audio and/or video data to telephone 74.

One advantage associated with IP telephones is their ability to communicate and interact with any other IP device coupled to the IP network. For example, IP telephones may interact and communicate with other IP telephones, with non-telephony IP devices, and even with virtual telephony devices. A virtual telephony device may be implemented as software, firmware and/or hardware to interact with devices in communication network 10. Virtual telephony devices may be implemented as software or firmware on any existing or dedicated device on the IP network. For example, computer 27 contains software for implementing one or more virtual telephony devices 28. Virtual telephony device software may also be located at call manager 26, or any other network device. The computer or other device on which the virtual telephony software is located includes a network interface, a memory to store the software, and a processor to execute the software.

Virtual telephony devices 28 may be logically inserted between two or more telephones to act as an intermediary between the two telephones. Once such a relationship is established, signaling and media streaming that passes through virtual telephony device 28 may then be modified through address translation or media stream manipulation for various reasons before they are sent on to the destination device. Reasons for such modifications include duplicating streams, dynamically redirecting streams,

maintaining connections between devices, converting between data formats (e.g., A-Law to μ-Law), and injecting media.

As will be described in the present application, one implementation of virtual telephony device 28 is as a telephony proxy to allow telecommunications between a trusted telephone coupled to a protected network, such as LAN 20, and an untrusted device external to the protected network while still maintaining network security. Through the use of an authentication controller 25, which evaluates incoming communications, the telephony proxy can be used to monitor communications directed to trusted telephones on LAN 20, for example, from untrusted devices outside of LAN 20 (e.g., telephones coupled to LAN 40 or Internet 50). The telephony proxy may also be used to manipulate the media streaming between the trusted telephone and the untrusted device as required to maintain the integrity of the protected network.

In order for a call to be placed through a virtual telephony device, for example a call placed to IP telephone 24a in LAN 20 through virtual telephony device 28, telephone 24a should be registered with virtual telephony device 28. Telephone 24a is instructed by call manager 26 to register with virtual telephony device 28 at a specified IP address and port. Telephone 24a signals virtual telephony device 28 via TCP/IP indicating that it would like to register. If virtual telephony device 28 accepts the registration request, telephone 24a sends a registration message to virtual telephony device 28 using TCP/IP. The registration message typically comprises information about the telephone such as the telephone's IP

and media access control (MAC) addresses, the type of telephone, and the codec(s) used by the telephone.

FIGURE 2 illustrates an exemplary communication link created using virtual telephony device 28. The communication link represents any connection or other coupling between two or more telephony devices that allows the telephony devices to communicate in some manner. It should also be noted that although the TCP and UDP protocols are specifically identified in the following discussion, any other suitable signaling and media transmission protocols may be used. Virtual telephony device 28 initiates this communication link by first creating a logical connection to telephone 24a. Creating this logical connection involves associating logical UDP and TCP ports of virtual telephony device 28 with telephone 24a. Virtual telephony device 28 designates a TCP port (for example, port 2000) as the signaling port of telephone 24a and designates a UDP port (for example, port 2100) as the streaming port of telephone 24a. Virtual telephony device 28 instructs call manager 26 to send all signaling directed to telephone 24a to logical port 2000 of virtual telephony device 28. Likewise, virtual telephony device 28 instructs call manager 26 to send all media streaming directed to telephone 24a from other telephones to logical port 2100 of virtual telephony device 28. Virtual telephony device 28 will automatically forward any data that is subsequently sent to these ports of virtual telephony device 28 to the IP address of telephone 24a (for example 200.50.10.1). As far as call manager 26 is concerned, telephone 24a is located at these logical ports of virtual telephony device 28.

Likewise, virtual telephony device 28 has typically designated a TCP port (for example, port 1000) as the signaling port of call manager 26 (data is typically not streamed to and from call manager 26, so a UDP port is usually not required). Virtual telephony device 28 instructs telephone 24a (as well as any other registered telephones) to send all signaling directed to call manager 26 to logical port 1000 of virtual telephony device 28.

In operation, when a call is placed to telephone 24a by another telephone 24b (which has registered with virtual telephony device 28 in a similar manner as telephone 24a), telephone 24b initially sends a call initiation request to call manager 26 indicating a desire to communicate with telephone 24a. This call initiation request is sent by telephone 24b to port 1000 of the IP address of virtual telephony device 28 (for example, 200.50.10.30). Virtual telephony device 28 then forwards the request to call manager 26. In order to establish the call, call manager 26 sends signaling information to telephone 24a at port 2000 of the IP address of virtual telephony device 28. Virtual telephony device 28 then forwards this signaling to telephone 24a. If telephone 24a accepts the call, call manager 26 establishes audio (and possibly video) streaming between telephones 24a and 24b by signaling telephone 24b to begin streaming data to port 2100 of virtual telephony device 28, and by signaling phone 24a to begin streaming to port 3100 of virtual telephony device 28. Thus a telecommunication link is established between telephones 24a and 24b using virtual telephony device 28.

When packets are received at port 2100, virtual telephony device 28 examines the packets and notes the

source address of the data. This source address is the IP address of telephone 24b, for example 200.50.10.2, and a particular logical port of this IP address. Virtual telephony device 28 then changes the source address and port in the header of the IP packets coming from telephone 24b to the IP address and logical UDP port of virtual telephony device 28 that was associated with telephone 24b when it registered with virtual telephony device 28 (for example, 200.50.10.30, port 3100). This address modification can be performed by an address modification module of virtual telephony device 28. Virtual telephony device 28 then forwards the packets to telephone 24a (this communication may be performed by a transmission module, such as a UDP/IP stack). Since the header of each packet indicates the media streaming originated from port 3100 of virtual telephony device 28, it appears to telephone 24a that telephone 24b is actually located at this address and port.

A similar process is performed when telephone 24a returns media streaming in response to the streaming from telephone 24b. Since it believes that telephone 24b is located at port 3100 of virtual telephony device 28, telephone 24a directs its data streaming to this location. When virtual telephony device 28 receives the IP packets at port 3100 (which it has previously associated with telephone 24b), it first changes the source IP address and port in the packets' header from the actual port and IP address (200.50.10.1) of telephone 24a to port 2100 of the IP address of virtual telephony device 28. Virtual telephony device 28 then forwards the packets to telephone 24b. Since the header of each packet indicates that the

media streaming originated from port 2100 of the IP address of virtual telephony device 28, it appears to telephone 24b that telephone 24a is actually located at this address and port. All subsequent data sent between telephones 24a and 24b is similarly passed through and modified by virtual telephony device 28.

Since all data that is sent between two IP telephones may be passed through virtual telephony device 28, virtual telephony device 28 can be used for other purposes in addition to the address translation function described above. For example, virtual telephony device 28 may serve as a telephony proxy to facilitate telecommunications between a "trusted device" located in the same network as the telephony proxy and an "untrusted device" located outside the network. In this case, communications between the trusted device and the untrusted device are routed through the telephony proxy after being authenticated.

For the purposes of this application the term "trusted device" will be used to indicate an IP telephone that is coupled to a protected or trusted IP network(s) being serviced by the telephony proxy, such as telephone 24b on LAN 20. The term "untrusted device" will be used to indicate an IP or non-IP device that is external to the protected IP network(s). The untrusted device may be coupled to an untrusted network, such as telephone 52 on Internet 50. Alternatively, the untrusted device may be a telephone coupled to a trusted network, such as telephone 32 on LAN 30. In this case, the telephone is untrusted to telephony proxy 28, for example, because the trusted network (LAN 30) is coupled to the protected network (LAN 20) using an untrusted network, such as Internet 50.

For simplicity, subsequent discussion will focus on telephony proxy 28, which is a type of virtual telephony device 28, being used to provide security to LAN 20. Therefore, LAN 20 is the protected (and trusted) network and telephones 24 coupled directly to LAN 20 are trusted telephones. However, it should be understood that telephony proxy 28 can be used in conjunction with any other type of network to which security needs to be provided.

Telephony proxy 28 operates like virtual telephony device 28, described in FIGURE 2, to facilitate a telephone call between two or more telephones. However, because at least one of the telephones is untrusted when telephony proxy 28 is used, an authentication step is required before a telecommunication link can be established between the telephones. This authentication step is performed by authentication controller 25. Thus, the primary difference between the telephony proxy software and the virtual telephony device software is that the telephony proxy software does not establish a telecommunication link between a trusted device and an untrusted device until authentication controller 25 approves the link.

When a call initiation request is made by an untrusted device to a trusted device (the term "trusted device" being used to indicate the target of a call initiation request before the request is authenticated), authentication controller 25 evaluates this request to determine if a telecommunication link should be established between the trusted device and the untrusted device using telephony proxy 28. Various methods of evaluating the call initiation request, such as an address look-up or a message format analysis, are described below in conjunction with FIGURE 3.

As with telephony proxy 28, authentication controller 25 may be implemented as software on any device in LAN 20. For example, the authentication software may be located on a dedicated computer, or it may be located on a computer having other purposes such as computer 26 running the call manager software or computer 27 running the telephony proxy software. In one embodiment, the call manager software, the authentication software, and the telephony proxy software may all be running on the same computer.

FIGURE 3 illustrates an exemplary method for using a virtual telephony proxy to facilitate a telephone call between a trusted device and an untrusted device. The method begins when a call initiation request is received from an untrusted device at step 102, indicating a desire to place a telephone call to a trusted device. For example, a call initiation request directed to telephone 24a may be generated by telephone 32 on LAN 30, and transmitted over Internet 50 to LAN 20. Alternatively, a call initiation request may be transmitted to LAN 20 from various other untrusted devices using WAN 60, PSTN 80, and/or ISP 90.

The call initiation request may comprise any indication that the untrusted device would like to communicate with a trusted device. LAN 20 may be configured such that all incoming call initiation requests are first directed to telephony proxy 28. Telephony proxy 28 may work in conjunction with or as part of a firewall 29 that is used to screen non-telephony data communications. In this case, incoming call initiation requests and other incoming telephony communications are directed to telephony proxy 28, and all other incoming communications are sent through firewall 29. Alternatively, incoming call initiation

requests may be sent to other initial destinations, such as call manager 26 (note that the call manager software may be running on the same computer as the telephony proxy software).

Once the call initiation request has been received, the request is transferred to authentication controller 25 at step 104. As described above, the authentication controller software may be running on the same computer as telephony proxy 28 and/or call manager 26, so this transferring step may simply involve passing the call initiation request between software modules on the same computer. The call initiation request is evaluated by authentication controller 25 at step 106. A variety of evaluations may be performed on the call initiation request to determine whether the request should be accepted and whether a call should be established between the untrusted device and the trusted device.

One such evaluation involves determining whether the trusted device is a proper recipient of a telephone call from an untrusted device. This evaluation may simply involve determining whether the trusted device is actually a telephone or some other telephony device capable of receiving telephone calls. Since IP telephony allows the integration of telephones and other network devices on the same IP network, care must be taken to ensure that unauthorized parties are not able to access secured data or send unwanted data, such as a virus, to the network.

By ensuring that the object of the call initiation request is a telephone or other telephony device, these worries are reduced. There is typically no sensitive data located on an IP telephone that an intruder could access.

Furthermore, if a virus is sent to an IP telephone after it is connected with the untrusted device, the IP telephone may simply attempt to "play" the incoming IP packets to the telephone's user. In this case, nothing will happen since the packets are not in a media format, such as an RTP stream. Also, the data in the incoming packets is not stored at the telephone (except for temporary buffering), and it is typically not accessed in a manner that would infect the telephone or the network with a virus or other unwanted data.

One way that authentication controller 25 can determine whether the trusted device is actually a telephone is by comparing the network address of the called device with the addresses on an address list 23 stored in the memory of the computer running the authentication controller software (or in the memory of any other network device). For example, the approved address list may contain the IP addresses of telephones and other telephony devices that are permitted to receive calls from untrusted devices. Alternatively, address list 23 list may contain the IP addresses of untrusted devices that are either authorized to communicate with trusted devices or that are prohibited from communicating with trusted devices. Address list 23 may contain either individual or subnet addresses.

Once authentication controller 25 has evaluated the call initiation request, it determines the appropriate action to take at step 108 based on whether the evaluation was positive or negative. If the evaluation is negative, for example, if the trusted device to which the call is directed is not actually a telephone or other proper recipient of an incoming call, then authentication

controller 25 denies the call initiation request at step 110. Once the request is denied, call manager 26 will not attempt to establish a telecommunication link between the untrusted device and the trusted device.

If the evaluation of the call initiation request is positive, then authentication controller 25 transmits a signal to call manager 26 authorizing a telephone call between the trusted device and the untrusted device at step 112. In response to this signal, call manager 26 establishes a telecommunication link between the trusted device and the untrusted device at step 114. This telecommunication link, as described above in conjunction with FIGURE 2, may be established such that all telecommunications between the trusted device and the untrusted device are communicated through telephony proxy 28.

Assuming that the trusted device is registered with telephony proxy 28 (as described above), call manager 26 instructs the untrusted device to begin media streaming to the logical port of telephony proxy 28 that has been associated with the trusted device. Additionally, call manager 26 instructs telephony proxy 28 to associate another of its logical ports with the untrusted device. In the manner described above, telephony proxy 28 changes the information in header of the packets incoming from the untrusted device by altering the source address and source port to the address of telephony proxy 28 and the logical port of telephony proxy 28 that was associated with the untrusted device (note that the address may be in the IP header and the port may be in the UDP or TCP header). Telephony proxy 28 then forwards the packets to the trusted

device, so that the packets appear to be sent from telephony proxy 28. A similar address translation process is performed on packets being sent from the trusted device to the untrusted device, as described above.

The continuous address translation by telephony proxy 28 ensures that all communications between the trusted device and the untrusted device are controlled by telephony proxy 28. Such continuous control prevents the untrusted device from determining the actual network address of the trusted device.

In one embodiment, telephony proxy 28 also continuously monitors the media streaming between the trusted device and the untrusted device at step 315. For example, telephony proxy 28 can ensure that the media streaming is in a recognized audio encoding format, such as G.711, G.723, or G.729. Telephony proxy 28 can also ensure that the communications between the trusted device and the untrusted device are, in fact, media streaming (or more specifically, RTP media streaming). Furthermore, any other appropriate methods of evaluating the media streaming, including appropriate techniques implemented by data firewalls, may also be used to monitor any unauthorized access to a network. If telephony proxy 28 determines at any point that suspect media streaming or other transmissions are occurring, telephony proxy 28 can manipulate or terminate the data streaming between the untrusted device and the trusted device. Once the telephone call between the trusted device and the untrusted devices is completed (or once suspect transmissions are detected), the telecommunication link is terminated at step 116.

Although the present invention has been described with several embodiments, a myriad of changes, variations, alterations, transformations, and modifications may be suggested to one skilled in the art, and it is intended that the present invention encompass such changes, variations, alterations, transformations, and modifications as fall within the spirit and scope of the appended claims.